Procedimiento Nº PS/00355/2010

RESOLUCIÓN: R/02615/2010

En el procedimiento sancionador PS/00355/2010, instruido por la Agencia Española de Protección de Datos a la entidad FONT- SALEM, S.L., vista la denuncia presentada por ***A.A.A.*** y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 27/10/2009, tuvo entrada en esta Agencia escrito de D. ***A.A.A.*** (en lo sucesivo el denunciante) en el que denuncia a la empresa **FONT-SALEM, S.L.** (en lo sucesivo FONT-SALEM) por llevar a cabo una auditoria informática en el ordenador que la empresa le había asignado, lo que sirvió de justificación para su despido disciplinario por uso abusivo de Internet, con las siguientes irregularidades: no había ningún tipo de prohibición en el uso privativo de Internet, no se había avisado ni solicitado su permiso ni el del comité de empresa, y se rastrearon las páginas web accedidas por él sin su conocimiento ni consentimiento.

SEGUNDO: Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

1.- El denunciante aporta copia de la carta de despido, de 13/03/2009, que le fue remitida por la empresa, en la que se detalla el número de accesos que determina como no autorizados, indicando el propio documento qué páginas de Internet fueron accedidas de forma no autorizada y el tema o el tipo de contenido de dichas páginas. Además, en el comunicado se indica incluso la existencia de intentos de acceso a otras páginas web que el servidor bloquea, de contenido para adultos o juegos y diversión.

La carta adjunta un informe automatizado de la auditoria, que consta de 66 páginas, donde se muestra un estudio de las páginas visitadas y su categorización (motores de búsqueda, música, juegos, financiero, salud y medicina, redes sociales, etc …) así como un listado de las direcciones visitadas y la fecha y hora del acceso.

2.- Se ha solicitado información y documentación a FONT-SALEM, en concreto:

a. Alcance y ámbito de la auditoria informática que se llevó a cabo entre enero y febrero de 2009 (personal de la empresa investigado, chequeos que fueron efectuados, personal que ha tenido acceso a los datos arrojados por la auditoria, etc),

b. Información sobre la auditoria que fue facilitada a los empleados y a los representantes sindicales. Fecha en que fue facilitada dicha información. Documentación que lo acredite.

c. Información facilitada a los empleados sobre la utilización de los medios de trabajo (ordenador, correo electrónico, Internet) para fines particulares,

Ante lo cual se ha recibido la siguiente contestación:

"1. Información y ámbito de la auditoria informática que se llevó a cabo entre enero y febrero de 2009 (personal de la empresa investigado, chequeos que fueron efectuados, personal que ha tenido acceso a los datos arrojados por la auditoría etc.)":

Para garantizar la correcta actividad de FONT-SALEM, los responsables de informática, dentro de sus funciones y de forma recurrente, verifican y auditan que no exista ninguna anomalía que ponga en riesgo los sistemas de la compañía o se incumplan las políticas de Sistemas de Información de FONT-SALEM. En particular, tal y como se hace constar en la carta de despido de fecha 11 de marzo de 2009, durante los meses de enero y febrero de 2009, FONT-SALEM llevó a cabo una verificación y auditoria informática que, por un lado, tenía como objeto revisar la seguridad de los sistemas y, por otro, detectar posibles anomalías en la utilización de los medios que pone a disposición de los empleados, todo ello destinado a asignar y optimizar de un modo más eficiente el uso de los recursos informáticos por parte de los empleados de FONT-SALEM.
En relación con lo anterior, en aras a la mayor claridad posible sobre la información y ámbito de la auditoria informática, nos remitimos a los hechos que el juez considera probados en la Sentencia 347/2009 (hecho probado nº 6), declarando que "La empresa realizó en los meses de enero y febrero procedimiento de auditoria interna en las redes de la información con el objeto de revisar la seguridad del sistema y detectar posibles anomalías en la utilización de los medios puestos a disposición de los empleados, cuyo informe fue entregado a la administración de personal de la empresa el día 10 de marzo. En concreto, y por lo que se refiere al ordenador utilizado por los Jefes de Turno en cuyo historial de acceso a Internet aparece una gran cantidad de entradas, se entregó a la administración de personal auditoria detallada del historial de accesos a Internet, que es el mismo que se adjuntó a la carta de despido entregada al trabajador".

"2. Información sobre la auditoria que fue facilitada a los empleados y a los representantes sindicales. Fecha en que fue facilitada dicha información. Documentación que lo acredite".

En relación a la documentación e información solicitada en el apartado 2 de la solicitud de información de la AEPD de fecha 2 de diciembre de 2009, interesa a esta parte destacar lo siguiente:

(i) En el momento en que los trabajadores se incorporan a la plantilla de FONT-SALEM se les informa y hace entrega del documento "Manual de Acogida", de lectura obligatoria y que, entre otras informaciones, contiene las Normas Internas relativas a los Sistemas de Información (apartado 5.3.2) que describen las facultades de control y auditoria sobre los Sistemas de Información que FONT-SALEM se reserva (vid apartado Cuarto posterior). Dicha documentación se encuentra asimismo colgada en la intranet de la compañía.
(ii) En la carta de despido (adjuntada como Documento nº 3) FONT SALEM procedió a informar sobre la auditoria realizada a Don... (el denunciante)*, con copia al delegado sindical y al comité de empresa de la compañía. En relación con lo anterior, destacar que, tal y como se recoge en la Sentencia del Tribunal Supremo de 26 de septiembre de 2007, dictada en un Recurso para la Unificación de Doctrina, el artículo 20.3 del Estatuto de los Trabajadores habilita al empleador para controlar los medios de comunicación electrónicos que en cada caso asigne a sus empleados para el desarrollo de sus funciones. En este sentido, la propia Sentencia 347/2009 de constante referencia establece respecto al tema que nos ocupa que "Ninguna violación de derechos fundamentales se ha producido, entonces, por parte del empresario en el control del cumplimiento por el trabajador de sus obligaciones laborales que le atribuye el art. 20.3 del Estatuto de los Trabajadores, lo que determina que, en este punto, el motivo de impugnación del despido formulado por el actor*

no merezca favorable acogida. Siendo irrelevante, por otro lado, con base en los mismos argumentos, el que la empresa no informara previamente al trabajador que se iba a efectuar procedimiento de auditoria interna en las redes de la información, pues además de que, como ya se ha dicho, tal procedimiento se efectuó a nivel general de todos los equipos informáticos de la empresa y con el objeto, no solo de detectar posibles anomalías en la utilización de los medios puestos a disposición de los empleados, sino también de revisar la seguridad del sistema, la doctrina jurisdiccional (STS de 26 de septiembre de 2007 citada) ha sentado el criterio de que en supuestos como el presente no resulta aplicable el art. 18 ET".

CUARTO. Apartado 3 de la solicitud de información de la AEPD

"3. Información facilitada a los empleados sobre la utilización de los medios de trabajo (ordenador, correo electrónico, Internet) para fines particulares".

Tal y como se ha comentado en el apartado Tercero anterior, FONT-SALEM facilita a todos sus empleados el documento "Manual de Acogida" en el que, entre otras informaciones, se facilitan las normas de Seguridad de los Sistemas de Información de las Empresas del Grupo Damm (apartado 5.3.2), que transcribimos a continuación:

"5.3.2 Seguridad de los Sistemas de Información de las Empresas del Grupo Damm
Los Sistemas de Información de la Empresa sólo deberán utilizarse para llevar a cabo tareas de negocio autorizadas por la Dirección. Su uso podrá ser auditable en cualquier momento.
El uso de los Sistemas de Información de la Empresa deberá atenerse siempre a unas normas éticas básicas. Estará prohibida su utilización para el tratamiento y distribución de material ofensivo o no apropiado.
Toda la información creada, almacenada o transmitida utilizando los Sistemas de Información de la Empresa es propiedad de la misma.
La Empresa podrá acceder a información almacenada o transmitida empleando sistemas de su propiedad y se reserva el derecho de vigilar sus sistemas con propósito de auditoria, para asegurar el uso adecuado y detectar violaciones de seguridad.
Los usuarios no deben suponer que las comunicaciones que realicen empleando los sistemas de la Compañía son privadas.
El DSI o el responsable de informática de cada una de las Empresas del Grupo Damm serán los únicos encargados de la instalación del software en los equipos del Grupo Damm. Debe recordar que, aunque se disponga de una licencia de uso válida para un determinado programa, es necesario que se encuentre en la lista de programas autorizados a ser instalados en un PC o estación de trabajo.

Para conectarse a los Sistemas de Información de las Empresas del Grupo Damm:

No suplante a otra persona. Utilice únicamente sus identificativos de usuario.
No conecte ningún dispositivo a los equipos de informática o de telecomunicaciones sin permiso del DSI o del responsable de informática de su Empresa.
La conexión no autorizada de sistemas v redes de las Empresas del Grupo Damm con los de entidades externas puede suponer la aparición de riesgos de seguridad de la información grave para dichas Empresas. Por esta razón este tipo de conexiones está prohibido si no existe la aprobación expresa del DSI o del responsable de informática de su Empresa. Este aspecto será controlado de forma estricta.
Si necesita acceder a Sistemas o Información externos a las Empresas del Grupo Damm, debe usar los recursos informáticos corporativos aprobados e instalados por el DSI o por el responsable de informática de su Empresa.

Los Sistemas de Información de Damm disponen de mecanismos de detección y eliminación de virus informáticos, si sospecha la presencia de un virus o el software antivirus le avisa de la existencia de un virus en un fichero el procedimiento a seguir es:

Salir del programa o documento que se esté utilizando cuanto antes, no intentando guardar los cambios en el documento. No intentar eliminarlo sino contactar inmediatamente con el DSI o el responsable de informática de su Empresa. No apagar el ordenador, pero tampoco seguir usándolo.

Si se recibe un mensaje advirtiendo de la peligrosidad de abrir un correo electrónico solicitando que se envíe el mensaje a todos los usuarios que se conozca, probablemente se trate de un falso virus. Ante un mensaje de este tipo, se debe avisar al DSI o al responsable de informática de su Empresa.

Se deben recordar los siguientes aspectos al conectarse con las Empresas del Grupo Damm u otras:

Internet es utilizado por millones de personas en todo el mundo. No todos los usuarios tienen intereses legítimos.
Se debe presumir que cualquier información no protegida (mediante cifrado, por ejemplo) que se envíe por Internet puede ser leída por personas a las que no iba dirigida.
No utilice modems ni otros sistemas de acceso a redes de datos o a Internet. En caso de necesidad, solicítelo al DSI.
El correo electrónico sólo deberá utilizarse para llevar a cabo tareas de negocio autorizadas por la Dirección. Utilice siempre las herramientas de correo electrónico homologadas por Damm. No utilice funciones de respuesta automática de correo para responderá los mensajes recibidos por Internet, ni envíe o reenvíe cartas encadenadas. Tampoco envíe correos masivos sin previa autorización DSI o CSU. "

TERCERO: Con fecha 03/02/2010, se dictó resolución por el Director de la Agencia Española de Protección de Datos, acordando el archivo de la denuncia reseñada en el Hecho Primero. Dicha resolución, fue notificada al recurrente en fecha 09/02/2010, según aviso de recibo que figura en el expediente.

CUARTO: El denunciante presentó, en fecha 08/03/2010, recurso de reposición, siendo la fecha de entrada en el Registro de esta Agencia Española de Protección de Datos, el 16/03/2010, fundamentándolo, básicamente, en que, si bien la resolución recurrida determinaba la legitimidad de la intervención por parte de los responsables de FONT-SALEM, de su ordenador de trabajo, en base, por un lado, a la sentencia del Juzgado de lo Social nº 5 de Valencia, que consideraba legítima dicha intervención; por otro, en razón a la actividad jurisprudencial del Tribunal Supremo, así como en la doctrina establecida a nivel tanto europeo como nacional a partir de los trabajos del Grupo de Berlín y de esta Agencia Española de Protección de Datos que determina que caben dichas intervenciones, previa comunicación a los trabajadores de dicha posibilidad; y por último, a lo alegado por la mercantil, en torno a que facilita un manual de acogida a los trabajadores al respecto de los usos de Internet en el trabajo y a la posibilidad de auditar los equipos de trabajo; el recurrente ha aportado resolución del Tribunal Superior de Justicia de la Comunidad Valenciana, que, en segunda instancia, y sobre los hechos denunciados ante el Juzgado de lo Social nº 5 de Valencia, ha reconocido la improcedencia de su despido, en base a la obtención ilícita de la prueba del mismo, la intervención de su equipo de trabajo, sin previa comunicación y afectando al derecho a la intimidad del trabajador. Además alega que nunca recibió dicho manual de acogida sobre usos de Internet, en la medida en que se incorporó a

dicho puesto en el año 1992, fecha en la que dicho servicio no se encontraba operativo en su centro de trabajo; y por otro lado se aportan certificaciones tanto de la Sección Sindical de CC.OO. como del Comité de Empresa de FONT SALEM, que declaran no haber tenido noticia anterior a la intervención del equipo del hoy recurrente, de rastreos previos de las páginas web visitadas por los trabajadores, ni de la existencia de una prohibición de navegar por Internet a los trabajadores.

Este recurso fue estimado por Resolución del Director de la Agencia Española de Protección de Datos, de fecha 07/04/2010, conforme a los siguientes fundamentos de derecho:

<<La resolución de esta Agencia Española de Protección de Datos, al expediente E/03490/2009 de 3 de febrero de 2010, se fundamentaba, en sus conclusiones, en la actividad doctrinal del Tribunal Supremo en torno a la afectación al derecho a la intimidad de los trabajadores en el ejercicio, por parte del empresario, de su derecho a verificar el cumplimiento, por parte de sus trabajadores, de sus deberes laborales, consagrado por el artículo 20 del Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores; todo ello puesto en relación con los trabajos, que al respecto, se han visto desarrollados por la Unión Europea a través de su "Grupo de Berlín" y por la propia actividad de esta Agencia Española de Protección de Datos.

Como quedaba de manifiesto en dicha resolución, en la actuación del empresario, en ejercicio de sus derechos de verificación, existe un conflicto con el derecho a la intimidad del trabajador y, por extensión, con el derecho a la protección de datos de carácter personal del mismo. Sin embargo, el derecho a la intimidad del trabajador no ha de considerarse como un derecho absoluto, sino que ha de valorarse de acuerdo a los condicionamientos que se encuentren presentes en su desarrollo. Así, se ha determinado jurisprudencialmente que, si bien los elementos aportados por el empresario a los trabajadores para el desarrollo de su actividad profesional han de constituirse como herramientas de trabajo y por tanto, han de ser empleados para el pleno desenvolvimiento de dicha actividad, no es menos cierto que existen ciertos usos sociales en torno a la utilización de determinados medios, como los ordenadores con conexión a Internet, que permiten un cierto ámbito de actuación, fuera del estricto cumplimiento de los deberes profesionales. Así, se ha venido estableciendo que, si bien dicho margen de actuación privada sobre los bienes de trabajo puede traducirse, en ocasiones, en actuaciones abusivas, es necesario que el empresario, previamente al inicio de la actividad sobre dichos bienes, establezca los límites en torno a la utilización de éstos e informe, previamente a los trabajadores, de las posibles intervenciones de comprobación que se pudieran desarrollar sobre los mismos.

En la resolución recurrida, en base a lo concluido por el Juzgado de lo Social nº 5 de Valencia, que admitió como prueba legítima, la auditoria sobre el equipo de trabajo del denunciante, y en base a lo manifestado por FONT SALEM S.L., en torno a la existencia de una previsión de intervención, conocida por los trabajadores, a partir de la existencia de un manual de acogida que se manifiesta sobre dichos términos, se determinó que, al menos en apariencia, se cumplían los requisitos establecidos jurisprudencial y doctrinalmente, como para entender que existía una habilitación para la intervención del equipo de trabajo del hoy recurrente, sin necesidad del consentimiento del mismo, y por tanto, se determinó la ausencia de infracción de la normativa en materia de protección de datos. Sin embargo, de acuerdo a lo aportado por el recurrente junto a su escrito de recurso, el Tribunal Superior de Justicia de la Comunidad Valenciana, ha llegado a una conclusión distinta en sede judicial, determinando que la empresa "no ha establecido previamente las reglas de uso de esos medios -con aplicación de prohibiciones absolutas o parciales- ni ha informado a los trabajadores de que se instauraría un control y de los medios que fuera a aplicar en orden a comprobar la corrección de los uso, así como de las medidas que se adoptarían en su caso para garantizar la efectiva utilización laboral

del medio informático", por lo que concluye que existe una violación del derecho a la intimidad del trabajador y determina que "la prueba debe reputarse ilícitamente obtenida". En base a dichas conclusiones conformadas en sede judicial, a lo que se adiciona lo manifestado por miembros tanto de la Sección Sindical de CC.OO en FONT SALEM, como de su comité de empresa, en referencia a la falta de una información previa en este sentido, ha de determinarse que se dan las condiciones para estimar el presente recurso, en la medida en que, en principio, no parece que FONT SALEM llevara a cabo la actuación de información previa a los trabajadores, que es requerida en el presente caso, por lo que, conforme a lo expuesto, se procede la estimación del recurso planteado y la realización de actuaciones previas de investigación tendentes al esclarecimiento de los hechos anteriormente expuestos>>.

QUINTO: Con fecha 07/07/2010, el Director de la Agencia de Protección de Datos acordó iniciar procedimiento sancionador a la entidad FONT SALEM por la presunta infracción del artículo 6.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal (en lo sucesivo LOPD), tipificada como grave en el artículo 44.3.d) de dicha norma, pudiendo ser sancionada con multa de 60.101,21 € a 300.506,05 €, de acuerdo con el artículo 45.2 de la citada Ley Orgánica.

SEXTO: Notificado el citado acuerdo de inicio de procedimiento sancionador, se recibe escrito de alegaciones de la entidad FONT-SALEM en el que ratifica el contenido del escrito de contestación al requerimiento de información de los Servicios de Inspección, que motivó el archivo de la denuncia formulada, y añade lo siguiente:

. El acuerdo de apertura del presente procedimiento estuvo motivado por el recurso de reposición interpuesto por el denunciante contra la resolución de archivo de 03/02/2010, del Director de la Agencia Española de Protección de Datos, que se fundamenta en que la Sentencia 483/2010 por la que se reconoce la improcedencia del despido del denunciante en base a la obtención ilícita de la prueba del mismo, la cual ha sido recurrida ante el Tribunal Supremo mediante recurso de casación para la unificación de doctrina, de fecha 05/05/2010, ya que la Sentencia de 05/06/2006 de la Sala de lo Social del Tribunal Superior de Justicia de Galicia es contradictoria en todo lo siguiente:

(i) Considerar que la prueba -aportada al proceso de despido del Denunciante- que acreditaba la utilización indebida, reiterada y desproporcionada de una herramienta de la empresa, en horas de trabajo, en lugar de cumplir con sus obligaciones profesionales, no es admisible por afectar a la intimidad del trabajador.

(ii) Considerar que la empresa no puede realizar una Auditoria de seguridad, realizada en el "servidor" de la empresa (no en el ordenador utilizado por el trabajador y otros compañeros suyos) que sólo descarga el "historial" de accesos a páginas de internet, por cuanto -al listar las páginas visitadas desde las diferentes terminales ("tráfico", no "contenido")-, se vulnera el derecho a la intimidad del trabajador.

(iii) Considerar que ese "hallazgo casual", a partir del cual se detecta un desmedido uso -no profesional- por medio de un ordenador compartido por varios trabajadores -pero en horarios diferentes- no legitimaba a la empresa a determinar la persona que habla "distraído" su deber laboral y se había dedicado a labores de "ocio" en tiempo de trabajo.

(iv) Considerar, en definitiva, que una utilización abusiva (no circunstancial) y permanente de una herramienta empresarial no puede ser imputada ya que -para ello- es preciso acreditar, al menos, los tiempos de acceso a páginas ajenas al trabajo, lo que conlleva (según la sentencia que impugnamos) la ilicitud del medio probatorio, convirtiendo en "inmune" al trabajador que dedica su tiempo de trabajo a "navegar" por internet. No estamos hablando del correo personal, ni de cualquier tipo de acceso a los contenidos generados por el trabajador, ni correspondencia, etc.. simplemente la constatación de que -en horas de trabajo- se utiliza el ordenador para otros Unes: mero "tráfico".

(v) La contradicción que se invoca se refiere a la determinación de los límites del control empresarial sobre un ámbito que, aunque vinculado al trabajo, puede afectar a la intimidad del

trabajador.

En síntesis, cada sentencia establece una "posición" jurídica opuesta. En la Sentencia 483/2010 un dato que existe en todos los ordenadores (no sólo los servidores centrales) como es el "historial" es decir, la mera relación de páginas en navegación (no contenidos ni, por supuesto, correos) con la exclusiva identificación del día, hora, duración y terminal utilizada, se considera vulneradora de los derechos consagrados en el artículo 18.3 de la CE., mientras que en la STSJ de Galicia se estima que es razonable -la actuación empresarial- y que en modo alguno el conocimiento del "historial" que es un dato existente en todos los ordenadores comporta violación de la intimidad del trabajador, al no penetrarse en el conocimiento de sus contenidos.

. FONT-SALEM, como todo empresario, tiene derecho al control del cumplimiento por el trabajador de sus obligaciones laborales, conforme el articulo 20.3 del Estatuto de los Trabajadores, por lo que procedió a realizar la Auditoria de sus sistemas, para de este modo detectar cualquier anomalía que pusiera en riesgo sus sistemas o se incumplieran las políticas de Sistemas de Información de la entidad, todo ello destinado a asignar y optimizar de un modo más eficiente el uso de los recursos informáticos por parte de los empleados. Esta actuación es legitima a la luz de la Sentencia del Tribunal Supremo de 26 de septiembre de 2007, que determina que el artículo 20.3 del Estatuto de los Trabajadores habilita al empleador para controlar los medios de comunicación electrónicos que en cada caso asigne a sus empleados para el desarrollo de sus funciones, tal y como es el caso que nos ocupa.

Asimismo, y de conformidad con la Sentencia del Tribunal Constitucional 98/2000 y 186/2000, los medios que se utilicen para ejercitas dichas facultades de control deben ser, en cualquier caso idóneos (adecuada para el fin previsto), necesarios (que sirva de prueba de la irregularidad cuya acreditación se persigue), equilibrados (que no violente en mayor medida de la necesaria los derechos del trabajador) y justificados (no caprichosos). A este respecto, considera FONT-SALEM que la Auditoria realizada es un medio idóneo y adecuado para controlar los medios de comunicación electrónicos; necesario porque tiene la capacidad de probar un uso inadecuado de los mismos; equilibrado, porque la Auditoria única y exclusivamente analiza el "historial" de accesos del terminal utilizado por el denunciante conjuntamente con otros trabajadores, no el contenido de las páginas web (URL) visitadas en horario de trabajo, v por tanto no "violenta" los derechos del trabajador; y justificado en tanto en cuanto la comprobación del buen uso y optimización de los sistemas no es un capricho del empresario sino de una obligación de todo buen empresario que repercute positivamente en todos los aspectos del negocio.

A más abundamiento, en el momento en que los trabajadores se incorporan a la plantilla de FONT-SALEM se les informa y hace entrega del documento "Manual de Acogida", de lectura obligatoria y que, entre otras informaciones, contiene las Normas Internas relativas a los Sistemas de Información (apartado 5.3.2) que describen las facultades de control y auditoria sobre los Sistemas de Información que FONT-SALEM se reserva. Dicha documentación se encuentra asimismo colgada en la intranet de FONT-SALEM a disposición de todos los empleados, por lo que no cabe alegar su desconocimiento por parte de los trabajadores que se incorporaron a la plantilla de FONT-SALEM con anterioridad a su aprobación.

Por todo lo anterior, considera que no ha vulnerado el derecho a la intimidad del denunciante, y que por tanto la excepción a la obtención del consentimiento establecida en el artículo 6.2 de la LOPD sería de aplicación plenamente.

. FONT-SALEM no ha vulnerado el derecho a la intimidad del denunciante. No ha accedido a los datos personales del mismo, ni a su correo electrónico ni a “su” ordenador. La auditoria trasladó

a la dirección de FONT-SALEM un listado (que formó parte de la carta de despido, que contiene el literal del histórico de las páginas web visitadas a través de un terminal que utilizaban los jefes de tumo, que señala exclusivamente los tiempos y las páginas visitadas en navegación, por lo que puede llegar a plantearse si esta información es un dato personal. La auditoria lo único que detecta es una *excesiva utilización,* desde un terminal conecto al servidor de la empresa, para actividades no relacionadas con el trabajo, desconociendo inicialmente y sin poder identificarlo al utilizarse un password común y "cuasi-público".

A partir de esa «utilización desmedida" y genérica (el historial del periférico, no del usuario, FONT-SALEM deduce y determina que ese uso indebido coincide en horario con la prestación de servicios del denunciante y, en concreto, con los espacios de tiempo en que no coincidía físicamente con otros empleados.

En síntesis de lo manifestado, no se vulnera la intimidad del trabajador por el hecho de que la empresa tenga conocimiento -no forzado- del historial de navegación en internet, siempre que no se acceda al contenido de las páginas ni, por supuesto, a los correos o datos propios del Denunciante. Dicho de otra forma, el derecho a la intimidad no puede alcanzar -por colisión- con el derecho del empleador al normal uso y utilización de sus medios operativos. Lo contrario inhabilita cualquier opción para viabilizar el derecho del empresario en el control natural de sus medios productivos.

Por todas estas razones, entiende FONT-SALEM que la Auditoria no vulneró el derecho a la intimidad del Denunciante, y por tanto la excepción a la obtención del consentimiento establecida en el artículo 6.2 de la LOPD sería de aplicación plenamente en la medida en que el tratamiento de la información relativa a la Auditoria es necesaria para el mantenimiento y cumplimiento de la relación laboral.

. Subsidiariamente, solicita la aplicación de lo dispuesto en el artículo 45.5 de la LOPD, con la imposición de una sanción por el importe previsto para las infracciones que preceden en gravedad en su grado mínimo, considerando que no ha existido culpa, en tanto en cuanto para garantizar la correcta actividad de FONT-SALEM, los responsables de informática, dentro de sus funciones y de forma recurrente, verifican y auditan que no exista ninguna anomalía que ponga en riesgo los sistemas de la compañía o se incumplan las políticas de Sistemas de Información de FONT-SALEM; se facilita a todos los empleados el documento "Manual de Acogida" citado, no se ha cometido reincidencia y los daños y perjuicios causados han sido escasos.

SÉPTIMO: En fecha 16/09/2010, se acordó por el Instructor del Procedimiento la apertura del período de práctica de pruebas, teniéndose por reproducidas a efectos probatorios la denuncia interpuesta y la documentación que acompaña, así como los documentos obtenidos y generados por los Servicios de Inspección ante FONT SALEM, el Informe de actuaciones previas de Inspección que forman parte del expediente E/01096/2010, la Resolución de archivo de actuaciones dictada por el Director de la Agencia Española de Protección de Datos en fecha 03/02/2010, el recurso interpuesto contra la misma por el denunciante y la Resolución del Director de la Agencia Española de Protección de Datos que estima dicho recurso. Por otra parte, se dieron por reproducidas a efectos probatorios, las alegaciones al acuerdo de inicio PS/00355/2010 presentadas por FONT SALEM y la documentación que a ellas acompaña.

OCTAVO: Con fecha 03/12/2010, se emitió propuesta de resolución en el sentido de que por el Director de la Agencia Española de Protección de Datos se sancione a FONT SALEM con multa de 60.101,21 (sesenta mil ciento un euros con veintiún céntimos), por la infracción del artículo 6.1 de la LOPD, tipificada como grave en el artículo 44.3.d) de dicha norma.

Notificada la citada propuesta, el plazo concedido a la entidad FONT SALEM para

formular alegaciones transcurre sin que se haya recibido escrito alguno.

HECHOS PROBADOS

PRIMERO: El denunciante prestó servicios como empleado en la empresa FONT-SALEM desde el 22/01/1992 hasta su despido disciplinario por falta muy grave, que tuvo lugar en fecha 13/03/2009. Dicho despido fue notificado al denunciante mediante escrito de la misma fecha, en el que se detallan los hechos que determinaron dicho acuerdo de la entidad FONT-SALEM. Concretamente, informan que durante los meses de enero y febrero de 2009 la empresa llevó a cabo una auditoria informática para revisar la seguridad del sistema y detectar las posibles anomalías de utilización de los medios puestos a disposición de los empleados, constatando que el denunciante, durante el período reseñado y en horas de trabajo, utilizó los accesos a Internet desde su terminal y con su clave para navegar y acceder a páginas ajenas a su trabajo y en número altamente desproporcionado por desmedido, hasta un total de 4669 accesos de uso o interés particular, del total de 5556 páginas visitadas.

A la carta de despido se acompañaron las 66 páginas del "Reporte de Auditoria Detallada del Utilizador", que muestra un estudio de las páginas visitadas y su categorización (motores de búsqueda, música, juegos, financiero, salud y medicina, redes sociales, etc…), así como un listado de las direcciones visitadas, fecha y hora de acceso.

SEGUNDO: Contra el despido reseñado en el Hecho Probado Primero, el denunciante interpuso demanda ante los Juzgados de Valencia, dando lugar a la Sentencia 347/2009, de 20/07/2009, del Juzgado de la Social número 5 de Valencia, en la que se declaran probados, entre otros, los siguientes hechos:

<<1.- El trabajador demandante... (el denunciante) ha prestado servicios para la empresa demandada FONT SALEM S.L. con la antigüedad reconocida de 22 de enero de 1992, categoría profesional...
2.- En fecha 13 de marzo de 2009 la empresa notificó al trabajador su despido disciplinario con efectos de esa misma fecha por los hechos que en la comunicación (a la que se acompaña, formando parte de los hechos imputados las 66 páginas del "reporte de auditoria detallada del utilizador") constan y que se dan por reproducidos en aras a la brevedad. Cuyos hechos constituyen, según la carta, falta muy grave conforme al art. 54.2.d) del Estatuto de los Trabajadores y al art. 33.3.1 del Convenio de empresa.
El día 12 de marzo anterior la empresa dio traslado de los hechos imputados al delegado sindical...
3. El actor ha venido prestando servicios para la empresa como Jefe de Turno Mantenimiento...
4.- Los Jefes de Turno disponen para su trabajo de un ordenador en el despacho, que utilizan en su respectivo turno y a cuyo uso acceden con una contraseña (no ha quedado acreditado si es la misma para los tres Jefes de Turno o cada uno de ellos dispone de una contraseña propia)...
5.- Durante los meses de enero y febrero de 2009 el actor prestó servicios en los turnos que a continuación se señalan...
6.- La empresa realizó en los meses de enero y febrero procedimiento de auditoria interna en las redes de la información con el objeto de revisar la seguridad del sistema y detectar posibles anomalías en la utilización de los medios puestos a disposición de los empleados, cuyo informe fue entregado a la administración de personal de la empresa el día 10 de marzo. En concreto, y por lo que se refiere al ordenador utilizado por los Jefes de Turno en cuyo historial de acceso a Internet aparece una gran cantidad de entradas, se entregó a la administración de personal auditoria detallada del historial de accesos a Internet, que es el mismo que se adjuntó a la carta

de despido entregada al trabajador.
7.- Del referido informe se desprende que desde el citado ordenador -en el periodo 3 de enero a 28 de febrero de 2009- se accedió a Internet en horas de trabajo ,con un total de 5.566 "visitas" a páginas referidas al mundo multimedia-vídeos, piratería informática, anuncios, televisión, contactos, etc. La gran mayoría de los accesos o visitas a Internet se produjeron en los turnos de trabajo del actor (ya se ha dicho que los tres jefes de turno que utilizan el ordenador no coinciden trabajando) y fueron, por tanto, realizadas por éste...
Los accesos concretos, con mención de la hora en que se produjeron, constan en el ya citado reporte de auditoria detallada acompañado a la carta de despido y se dan por reproducidos en aras a la brevedad...>>.

Dicha Sentencia desestimó la demanda presentada por el denunciante, declarando procedente el despido objeto de enjuiciamiento.

TERCERO: Contra la Sentencia 347/2009, de 20/07/2009, del Juzgado de la Social número 5 de Valencia, el denunciante interpuso recurso de suplicación ante el Tribunal Superior de Justicia de la Comunidad Valenciana, que dictó Sentencia en fecha 16/02/2010 estimatoria del recurso, por lo que revoca la Sentencia recurrida y declara improcedente el despido de fecha 13/03/2009, en base a la obtención ilícita de la prueba del mismo, la intervención de su equipo de trabajo, sin previa comunicación y afectando al derecho a la intimidad del trabajador.

En esta Sentencia de fecha 16/02/2010 se determina que la entidad FONT-SALEM *"no ha establecido previamente las reglas de uso de esos medios -con aplicación de prohibiciones absolutas o parciales- ni ha informado a los trabajadores de que se instauraría un control y de los medios que fuera a aplicar en orden a comprobar la corrección de los uso, así como de las medidas que se adoptarían en su caso para garantizar la efectiva utilización laboral del medio informático"*, por lo que concluye que existe una violación del derecho a la intimidad del trabajador y determina que *"la prueba debe reputarse ilícitamente obtenida".*

CUARTO: El denunciante aportó declaraciones suscritas por el Delegado Sindical de Comisiones Obreras y de los miembros del Comité de Empresa de FONT SALEM, en las que manifiestan no haber tenido noticia anterior a la intervención del equipo del denunciante, de rastreos previos de las páginas web visitadas por los trabajadores, ni de la existencia de una prohibición de navegar por Internet a los trabajadores.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37.g) en relación con el artículo 36 de la LOPD.

II

En el presente caso se analiza, desde el punto de vista de la normativa de protección de datos de carácter personal, la conducta de FONT SALEM por la utilización de información relativa al historial de accesos a Internet realizados por el denunciante durante los meses de enero y febrero de 2009, en horas de trabajo y desde el terminal facilitado por dicha entidad al mismo, en su condición de empleado de aquella entidad y para el desarrollo de sus tareas como tal. Dicha información se contiene en 66 páginas del "Reporte de Auditoria Detallada del Utilizador", que muestra un estudio de las páginas visitadas y su categorización (motores de búsqueda, música,

juegos, financiero, salud y medicina, redes sociales, etc…), así como un listado de las direcciones visitadas, fecha y hora de acceso.

La primera cuestión que es preciso determinar es si la información tratada por FONT SALEM, asociada al denunciante, constituye datos de carácter personal.

El artículo 1 de la LOPD dispone: "La presente Ley Orgánica tiene *por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".*

En cuanto al ámbito de aplicación de la citada norma el artículo 2.1 de la misma señala: *"La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado"*; definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la citada Ley Orgánica 15/1999, como *"Cualquier información concerniente a personas físicas identificadas o identificables"*, añadiendo el apartado 1.f) del artículo 5 del Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD), que dato de carácter personal es *"cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables"*.

La definición de persona identificable aparece en la letra o) del citado artículo 5.1 del RLOPD, que considera como tal *"toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados"*.

En este mismo sentido se pronuncia el artículo 2.a) de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, según el cual, a efectos de dicha Directiva, se entiende por dato personal *"toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social"*. Asimismo, el Considerando 26 de esta Directiva se refiere a esta cuestión señalando que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a aquélla.

También en lo que se refiere al concepto de datos personales, cabe mencionar la Recomendación 1/2001, sobre datos de evaluación de los trabajadores, adoptada por el Grupo del Artículo 29 órgano consultivo independiente de la UE sobre protección de los datos y la vida privada, creado en virtud de lo previsto en el citado artículo de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Señala dicha Recomendación que:

"Según la definición incluida en la letra a) del artículo 2 de la Directiva 95/46/CE, los datos personales son toda información sobre una persona física identificada o identificable, tal como los datos relacionados con su identidad física, fisiológica, psíquica, económica, cultural o social.

El alcance de dicha definición implica que los datos personales incluyen, además de los datos de los registros de población o información resultante de factores objetivos que se pueden verificar o rectificar, cualquier otro elemento, información o circunstancia que incluya un contenido informativo tal que se sume al conocimiento de una persona identificada o identificable.

Así, se pueden encontrar datos personales en evaluaciones y juicios subjetivos que, en realidad, podrían incluir elementos específicos de la identidad física, fisiológica, psíquica, económica, cultural o social de los interesados. Esto sucede igualmente si un juicio o evaluación se resume en una puntuación o clasificación, o si se expresa mediante otros criterios de evaluación".

En este mismo sentido, el Dictamen 4/2007 del Grupo de trabajo del artículo 29, sobre el concepto de datos personales señala que *"un dato se refiere a una persona si hace referencia a su identidad, sus características o su comportamiento o si esa información se utiliza para determinar o influir en la manera en que se la trata o se la evalúa"*. Así para considerar "que los datos versan sobre una persona, debe haber un elemento "contenido", o un elemento "finalidad" o un elemento "resultado". "

Por consiguiente para determinar si nos encontramos ante un tratamiento de datos personales habrá que acudir a cada caso en concreto para ver si se produce alguna de las circunstancias citadas por el grupo de trabajo del artículo 29.

Si del análisis anterior se concluye que nos encontramos ante datos de carácter personal, será de aplicación la LOPD, entre cuyos principios debe mencionarse, en primer lugar el relativo a la necesidad de legitimación para efectuar el tratamiento de dichos datos, así como la calidad, especialmente en sus aspectos de finalidad y proporcionalidad del tratamiento.

Atendiendo a la definición contenida en las normas citadas, la información relativa al historial de accesos a Internet asociada a una persona identificada o identificable, que permite la evaluación de la misma o su comportamiento y repercute en los derechos y los intereses de la misma, da lugar a la consideración de dicha información como un dato personal incluido en el ámbito de aplicación de la normativa citada.

Así, en el presente supuesto, considerando que la información sobre los accesos a Internet se asocia al denunciante, debe concluirse la existencia de datos de carácter personal y la plena aplicabilidad de los principios y garantías expuestos en la normativa de protección de datos de carácter personal.

Ahora bien, aunque las personas tienen el poder de decisión sobre sus datos personales, no se trata de un derecho absoluto, sino que debe ceder llegado el caso ante la prevalencia de otros derechos y libertades también constitucionalmente reconocidos y protegidos. En el presente caso, en el que el tratamiento de los datos del denunciante se efectúa en el ámbito de una relación laboral, ha de ponderarse el derecho a la protección de los datos con el derecho reconocido a los empresarios para la vigilancia y control del cumplimiento de los deberes laborales que corresponden al trabajador.

III

El artículo 6 de la LOPD, referido al consentimiento en materia de protección de datos, establece en su punto 1º, la necesidad de la existencia de un consentimiento, por parte del titular del dato, para el tratamiento de sus datos personales por terceros. Así, dicho artículo es del tenor siguiente:

"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa."

Sin embargo, dicha capacidad de control sobre el tratamiento de datos por parte del titular de los mismos, no es absoluta, como determina el punto 2º del mismo artículo 6, que es del tenor siguiente:

"2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado"

De acuerdo a lo anterior, en el seno de una relación laboral, existe una suerte de habilitación legal para el tratamiento de datos de los sujetos de dicha relación, dentro de los términos de la misma. A esto ha de unirse lo previsto en el artículo 20.3 del Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, que, referido a la facultad de Dirección y Control de la Actividad Laboral por parte del empresario, nos dice:

"El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso".

Lo anterior confiere al empresario la capacidad para el control de la actividad de los empleados, pero ha de tenerse en cuenta que dicha circunstancia no implica la posibilidad de un tratamiento indiscriminado de los datos de los empleados, sin necesidad de consentimiento, sino que dicha posibilidad habría de acotarla dentro de los márgenes que la normativa y jurisprudencia entienda como legítimos, en orden del pacífico desarrollo de la relación laboral que justifica el tratamiento de datos, salvaguardando en todo caso el derecho a la dignidad del trabajador.

En el presente caso, el denunciante pone de manifiesto una actuación empresarial que entiende supone una vulneración de su derecho a la protección de datos de carácter personal, al haber procedido al acceso a su ordenador de empresa, sin mediar consentimiento del afectado, ni información previa al mismo ni a los representantes de los trabajadores, accediendo a los archivos temporales de su ordenador y al resto de información residida en el mismo. En este punto hemos de estudiar la normativa que se ha venido desarrollando en torno al tratamiento de datos en el seno de una relación laboral.

IV

El artículo 3.a de la LOPD define "*dato de carácter personal*" como: "*cualquier información concerniente a personas físicas identificadas o identificables.*" Por su parte, el Tribunal Constitucional, en su sentencia 292/2000, de 30 de noviembre ha establecido el carácter autónomo del derecho fundamental a la protección de datos de carácter personal, sobre el derecho a la intimidad, articulándose como un poder de control y disposición de los individuos al

respecto de sus datos personales, lo que faculta a la persona titular de los mismos, para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, pero dentro del contexto de la relación en la que se enmarca el referido tratamiento de datos, lo cual es aplicable al tratamiento de datos dentro del ámbito de las relaciones laborales.

La Unión Europea, a través del denominado "*Grupo de Berlín*", constituido en el seno de la Conferencia Internacional sobre Protección de Datos elaboró, en Agosto de 1996, el "*Informe y Recomendaciones sobre las Telecomunicaciones y la Privacidad en las relaciones laborales*", donde enmarcaba dentro del ámbito de protección de la normativa en materia de protección de datos el tratamiento de datos personales en el seno de una relación profesional. Analiza dicho informe los riesgos inherentes al control y vigilancia de los empleados a través de las modernas Tecnologías de la Información y Comunicaciones y las implicaciones de dichos controles con el ámbito de privacidad del empleado. Así, el Grupo de Berlín, desarrollo una serie de recomendaciones ante la legítima práctica de control empresarial sobre la actividad laboral de los empleados, para evitar intrusiones no justificables, en la esfera de intimidad del empleado, estableciendo que "*tanto los trabajadores como sus representantes deberán ser informados del tipo de tecnología utilizada por el empresario en relación con la vigilancia y seguimiento de su actividad laboral, debiendo abstenerse el empleador de recoger datos personales que resulten excesivos en razón de la propia naturaleza de la relación laboral*". El Grupo de Berlin ha determinado que "*el control deberá ser una respuesta proporcionada del empresario ante riesgos potenciales, teniendo en cuenta el derecho a la vida privada y otros intereses de los trabajadores*"

También es relevante en dicha materia la Recomendación(89) 2 del Consejo de Europa, en la que se establecen una serie de consideraciones en torno a las condiciones de tratamiento de los datos de los trabajadores en el ámbito de la relación laboral, estableciendo que solamente con el consentimiento del interesado o bien a partir de otras garantías previstas en el Derecho interno, podrían realizarse pruebas, análisis o procedimientos, destinados a evaluar el carácter o personalidad de una persona en el seno de dichas relaciones.

Como hemos visto, nuestro derecho interno, a través del artículo 20.3 del Estatuto de los Trabajadores, ha previsto la posibilidad de que el empresario, en aras de vigilar el desarrollo de la actividad laboral, pueda ejercer las actividades de control que les sean propias, pero, como se ha manifestado, las mismas han de sujetarse a una serie de limitaciones, que garanticen asimismo, los derecho de los trabajadores. El denunciante manifiesta que se accedió al ordenador de la empresa sin informar al trabajador ni a los representantes sindicales. Lo anterior, junto a lo visto en torno a las recomendaciones del Grupo de Berlín, puede ponerse en relación con lo establecido en el artículo 18 del Estatuto de los Trabajadores, que nos dice:

"Sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo. En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible."

El Tribunal Supremo, a través de sentencias, como la dictada el 26/09/2007 del Tribunal Supremo ante Recurso de Casación para la unificación de doctrina (966/2006) ha establecido una serie de consideraciones al respecto de los temas planteados, que han de ser tenidas en cuenta en el presente caso. Así, partimos de la capacidad del empresario para la vigilancia y control de la actividad laboral del artículo 20 del Estatuto de los Trabajadores, y el requisito

establecido por el artículo 18 del mismo cuerpo legal, de información y presencia de los representantes de los trabajadores en las actuaciones de control de sus efectos particulares en el centro de trabajo. La Sentencia aludida, a este respecto nos dice:

"La cuestión debatida se centra, por tanto, en determinar si las condiciones que el artículo 18 del Estatuto de los Trabajadores establece para el registro de la persona del trabajador, su taquilla y sus efectos personales se aplican también al control empresarial sobre el uso por parte del trabajador de los ordenadores facilitados por la empresa. Pero el problema es más amplio, porque, en realidad, lo que plantea el recurso, desde la perspectiva de ilicitud de la prueba obtenida vulnerando los derechos fundamentales (artículo 91.1 de la Ley de Procedimiento Laboral), es la compatibilidad de ese control empresarial con el derecho del trabajador a su intimidad personal (artículo 18.1 de la Constitución [RCL 1978, 2836]) o incluso con el derecho al secreto de las comunicaciones (artículo 18.3 de la Constitución Española), si se tratara del control del correo electrónico. El artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos (RCL 1999, 1190, 1572) establece también que toda persona tiene derecho al respeto de la vida privada y familiar y prohibe la injerencia que no esté prevista en la Ley y que no se justifique por razones de seguridad, bienestar económico, defensa del orden, prevención de las infracciones penales, protección de la salud, de la moral o de los derechos y libertades de los demás. (…) En el caso del uso por el trabajador de los medios informáticos facilitados por la empresa pueden producirse conflictos que afectan a la intimidad de los trabajadores, tanto en el correo electrónico, en el que la implicación se extiende también, como ya se ha dicho, al secreto de las comunicaciones, como en la denominada «navegación» por Internet y en el acceso a determinados archivos personales del ordenador. Estos conflictos surgen porque existe una utilización personalizada y no meramente laboral o profesional del medio facilitado por la empresa. Esa utilización personalizada se produce como consecuencia de las dificultades prácticas de establecer una prohibición absoluta del empleo personal del ordenador –como sucede también con las conversaciones telefónicas en la empresa– y de la generalización de una cierta tolerancia con un uso moderado de los medios de la empresa. Pero, al mismo tiempo, hay que tener en cuenta que se trata de medios que son propiedad de la empresa y que ésta facilita al trabajador para utilizarlos en el cumplimiento de la prestación laboral, por lo que esa utilización queda dentro del ámbito del poder de vigilancia del empresario, que, como precisa el artículo 20.3 del Estatuto de los Trabajadores, implica que éste «podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales», aunque ese control debe respetar «la consideración debida» a la «dignidad» del trabajador."
"(…)Tanto la persona del trabajador, como sus efectos personales y la taquilla forman parte de la esfera privada de aquél y quedan fuera del ámbito de ejecución del contrato de trabajo al que se extienden los poderes del artículo 20 del Estatuto de los Trabajadores. Por el contrario, las medidas de control sobre los medios informáticos puestos a disposición de los trabajadores se encuentran, en principio, dentro del ámbito normal de esos poderes: el ordenador es un instrumento de producción del que es titular el empresario «como propietario o por otro título» y éste tiene, por tanto, facultades de control de la utilización, que incluyen lógicamente su examen. Por otra parte, con el ordenador se ejecuta la prestación de trabajo y, en consecuencia, el empresario puede verificar en él su correcto cumplimiento, lo que no sucede en los supuestos del artículo 18"
(…) el hecho de que el trabajador no esté presente en el control no es en sí mismo un elemento que pueda considerarse contrario a su dignidad".

Por tanto, los soportes informáticos facilitados por el empresario a los trabajadores se erigen como bienes de empresa sobre los que el empresario puede ejercer su actividad de control, que ha de ser diferenciado de los efectos personales de los trabajadores y, por tanto, sobre los que no se les aplican los requisitos que establece el artículo 18 del Estatuto de los

Trabajadores. La sentencia aludida refuerza la capacidad de vigilancia sobre los soportes informáticos, al establecer:

"El empresario tiene que controlar el uso del ordenador, porque en él se cumple la prestación laboral y, por tanto, ha de comprobar si su uso se ajusta a las finalidades que lo justifican, ya que en otro caso estaría retribuyendo como tiempo de trabajo el dedicado a actividades extralaborales. Tiene que controlar también los contenidos y resultados de esa prestación. Así, nuestra sentencia de 5 de diciembre de 2003 (RJ 2004, 313) , sobre el telemarketing telefónico, aceptó la legalidad de un control empresarial consistente en la audición y grabación aleatorias de las conversaciones telefónicas entre los trabajadores y los clientes «para corregir los defectos de técnica comercial y disponer lo necesario para ello»".

En iguales términos se manifestó la Sentencia del Juzgado de lo Social nº 5 de Valencia (347/2009) en torno a la demanda presentada por el denunciante contra FONT SALEM, que concluyó con la no existencia de actividad infractora por parte de FONT SALEM en la falta de participación del denunciante y de los representantes sindicales en la actividad de auditoria realizada por la entidad.

Pese a todo lo anterior, tanto la jurisprudencia del Tribunal Supremo como el gabinete jurídico de esta Agencia de Protección de Datos, a través del informe jurídico 0247/2008, siguiendo las recomendaciones antes vistas, que a nivel europeo realizó el Grupo de Berlín, reconocen la necesidad de una actividad informativa por parte del empresario de la posible actuación intrusiva de comprobación del empleo de las herramientas informáticas facilitadas a los trabajadores. Así la referida sentencia de 26 de septiembre de 2007, a este respecto nos dice:

"En este punto es necesario recordar lo que ya se dijo sobre la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio. Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios –con aplicación de prohibiciones absolutas o parciales– e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones. De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado «una expectativa razonable de intimidad» en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (TEDH 1997, 37) (caso Halford) y 3 de abril de 2007 (TEDH 2007, 23) (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo par la protección de los derechos humanos (RCL 1999, 1190, 1572)".

En definitiva corresponde a la empresa decidir si autoriza a su personal a navegar con dichos fines y, en caso afirmativo, en qué medida se tolera esta utilización privada. Además, se ha determinado jurisprudencialmente que, si bien los elementos aportados por el empresario a los trabajadores para el desarrollo de su actividad profesional han de constituirse como

herramientas de trabajo y por tanto, han de ser empleados para el pleno desenvolvimiento de dicha actividad, no es menos cierto que existen ciertos usos sociales en torno a la utilización de determinados medios, como los ordenadores con conexión a Internet, que permiten un cierto ámbito de actuación, fuera del estricto cumplimiento de los deberes profesionales. Así, se ha venido estableciendo que, si bien dicho margen de actuación privada sobre los bienes de trabajo puede traducirse, en ocasiones, en actuaciones abusivas, es necesario que el empresario, previamente al inicio de la actividad sobre dichos bienes, establezca los límites en torno a la utilización de éstos e informe, previamente a los trabajadores, de las posibles intervenciones de comprobación que se pudieran desarrollar sobre los mismos.

En el presente caso, en base a lo concluido por el Juzgado de lo Social nº 5 de Valencia, que admitió como prueba legítima, la auditoria sobre el equipo de trabajo del denunciante, y en base a lo manifestado por FONT SALEM, en torno a la existencia de una previsión de intervención, conocida por los trabajadores, a partir de la existencia de un manual de acogida que se manifiesta sobre dichos términos, podría pensarse que se cumplían los requisitos establecidos jurisprudencial y doctrinalmente, como para entender que existía una habilitación para la intervención del equipo de trabajo del denunciante, sin necesidad del consentimiento del mismo. Sin embargo, el Tribunal Superior de Justicia de la Comunidad Valenciana llegó a una conclusión distinta en sede judicial, determinando que la empresa *"no ha establecido previamente las reglas de uso de esos medios- con aplicación de prohibiciones absolutas o parciales- ni ha informado a los trabajadores de que se instauraría un control y de los medios que fuera a aplicar en orden a comprobar la corrección de los uso, así como de las medidas que se adoptarían en su caso para garantizar la efectiva utilización laboral del medio informático"*, por lo que concluye que existe una violación del derecho a la intimidad del trabajador y determina que "*la prueba debe reputarse ilícitamente obtenida*". En base a dichas conclusiones conformadas en sede judicial, a lo que se adiciona lo manifestado por miembros tanto de la Sección Sindical de Comisiones Obreras en FONT SALEM, como por los miembros de su Comité de Empresa, en referencia a la falta de una información previa en este sentido, ha de determinarse que no se dieron las condiciones para que FONT SALEM pudiera acceder y utilizar la información relativa al historial de visitas a Internet efectuado por el denunciante y que motivó su denuncia.

A este respecto, no consta que FONT SALEM llevara a cabo la actuación de información previa a los trabajadores, que es requerida en el presente caso, por lo que, conforme a lo expuesto, se concluye que la citada entidad trató los datos personales del denunciante sin su consentimiento y sin que se de ninguna de las circunstancias que eximen de obtener el mismo, conforme a lo establecido en el artículo 6.2 de la LOPD. La intervención en el ordenador facilitado por la empresa al denunciante, en las condiciones expresadas afecta a su intimidad y supone una actividad infractora de la normativa en materia de protección de datos.

V

El artículo 44.3.d) de la LOPD tipifica como infracción grave: *"Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave"*.

El principio del consentimiento se configura como principio básico en materia de protección de datos y así se declara en la doctrina de la citada Sentencia del Tribunal Constitucional (STC 292/2002). Este principio se recoge, según ha quedado expuesto, en el artículo 6 de la LOPD, que exige la necesidad de consentimiento del afectado para que puedan tratarse sus datos de carácter personal.

La Audiencia Nacional ha manifestado, en su Sentencia de 22/10/2003, que *"... la descripción de conductas que establece el artículo 44.3.d) de la Ley Orgánica 15/1999 cumple las exigencias derivadas del principio de tipicidad, a juicio de esta Sala, toda vez que del expresado precepto se desprende con claridad cual es la conducta prohibida. En efecto, el tipo aplicable considera infracción grave "tratar de forma automatizada los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la Ley", por tanto, se está describiendo una conducta –el tratamiento automatizado de datos personales o su uso posterior- que precisa, para configurar el tipo, que dicha conducta haya vulnerado los principios que establece la Ley Orgánica. Ahora bien, estos principios no son de aquellos que deben inferirse de dicha regulación legal, sino que aparecen claramente determinados y relacionados en el título II de la Ley, concretamente, por lo que ahora interesa, en el artículo 6 se recoge un principio que resulta elemental en la materia, que es la necesidad de consentimiento del afectado para que puedan tratarse automatizadamente datos de carácter personal. Por tanto, la conducta ilícita por la que se sanciona a la parte recurrente como responsable del tratamiento consiste en usar datos sin consentimiento de los titulares de los mismos..."*.

En este caso, FONT SALEM ha incurrido en la infracción descrita en el citado artículo 44.3.d), toda vez que supone una vulneración del principio de consentimiento, consagrado en el artículo 6 de la LOPD, el tratamiento que ha realizado de los datos del denunciante sin su consentimiento y sin que concurra ninguna de las causas de exclusión del consentimiento recogidas en el apartado 2 del mencionado artículo 6.

VI

El artículo 45.1, 2, 4 y 5 de la LOPD establece lo siguiente:

"1. Las infracciones leves serán sancionadas con multa de 601,01 € a 60.101,21 €.
2. Las infracciones graves serán sancionadas con multa de 60.101,21 € a 300.506,05 €".
"4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.
5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate".

Considerando las circunstancias concurrentes, procede analizar la posibilidad de aplicar en el presente caso la previsión contenida en el artículo 45.5, que admite la imposición de la sanción prevista para las infracciones leves. A este respecto, la Sentencia de 21/01/2004 de la Audiencia Nacional, en su recurso 1939/2001*, señaló que* dicho precepto <<*…no es sino manifestación del llamado principio de proporcionalidad (artículo 131.1 de la LRJPAC), incluido en el más general del prohibición de exceso, reconocido por la jurisprudencia como principio general del Derecho. Ahora bien, la presente regla debe aplicarse con exquisita ponderación y sólo en los casos en los que la culpabilidad y la antijuridicidad resulten sustancialmente atenuadas, atendidas las circunstancias del caso concreto. Lo cual insistimos puede darse, por excepción, en casos muy extremos (de aquí la expresión "especialmente cualificada") y concretos"*.

En el presente procedimiento, atendidas las circunstancias expuestas, y, especialmente, que la entidad FONT SALEM conocía que el control realizado al ordenador utilizado por el denunciante, para obtener la información relativa al historial de accesos a Internet efectuados por el mismo durante enero y febrero de 2009, se llevó a cabo sin el conocimiento previo por parte del denunciante y sin haber informado sobre las posibilidades de utilización de los medios puestos a disposición de los trabajadores, no cabe apreciar una disminución cualificada de la culpabilidad en los hechos imputados, por lo que no procede aplicar lo dispuesto en el citado artículo 45.5 de la LOPD.

Teniendo en cuenta los criterios de graduación de las sanciones previstos en el artículo 45.4 y 5 de la LOPD y, en especial, la falta de intencionalidad apreciada en el presente caso y el volumen de tratamientos, procede la imposición a FONT SALEM de la sanción establecida para las infracciones graves en su cuantía mínima.

Vistos los preceptos citados y demás de general aplicación,

El Director de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: **IMPONER** a la entidad FONT- SALEM, S.L., por una infracción del artículo 6.1 de la LOPD, tipificada como grave en el artículo 44.3.d) de dicha norma, una multa de 60.101,21 € (sesenta mil ciento un euros con veintiún céntimos), de conformidad con lo establecido en el artículo 45.2 y 4 de la citada Ley Orgánica.

SEGUNDO: **NOTIFICAR** la presente resolución a FONT- SALEM, S.L. y a ***A.A.A.***.

TERCERO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida nº 0182 2370 43 0200000785 abierta a nombre de la Agencia Española de Protección de Datos en el Banco Bilbao Vizcaya Argentaria, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo. Si recibe la notificación entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si recibe la notificación entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del

referido texto legal.

Madrid, 30 de diciembre de 2010
EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: Artemi Rallo Lombarte